CLAIMS

1. An antifraud method comprising randomizing a physical signature of an integrated circuit executing a main program, comprising providing in said main program a branch to a randomly-chosen address of a sub-program having at least a features that any operation code that it contains directly or indirectly leads to an instruction included in the same sub-program except for at least one instruction for returning to the main program, and that whatever the input address in this sub-program, the execution of said instruction for returning returns to the main calling program at the instruction immediately following the instruction having caused said branching to the sub-program, to randomize a total execution time of the main program.

2. The method of claim 1, wherein the sub-program has a feature that whatever the input address in this sub-program, the instruction for returning to the main calling program is necessarily reached.

3. The method of claim 1, wherein said sub-program has a feature of containing no interrupt-generating operating code.

4. The method of claim 1, wherein said sub-program has a feature of containing no instruction for jumping or branching to an address external to said sub-program.

5. The method of claim 1, wherein said sub-program has a feature of containing no infinite loop.

6. The method of claim 1, wherein said sub-program is placed, with the code of the main program, in a ROM.

7. An integrated circuit for executing a deterministic program, comprising means for executing the antifraud method of claim 1.

8. An antifraud method for an integrated circuit executing a main program,

comprising:

branching or jumping from the main program to a randomly-selected address in a sub-program; and

executing the sub-program from the randomly-selected address to an instruction for returning to the main program.

9. A method a defined in claim 8, further comprising resuming execution of the main program after returning from the sub-program.

10. A method as defined in claim 8, wherein the sub-program contains no instruction for jumping or branching to an address external to the sub-program, except for the instruction for returning to the main program.

11. A method as defined in claim 8, wherein the sub-program contains no infinite loop.

12. A method as defined in claim 8, wherein the sub-program contains no interrupt-generating code.

13. A method as defined in claim 8, wherein any code in the sub-program leads directly or indirectly to the instruction for returning to the main program.

14. A method as defined in claim 8, wherein executing the sub-program comprises jumping or branching to a second sub-program and executing the second sub-program to the instruction for returning to the main program.

15. An antifraud method for an integrated circuit executing a main program, comprising:

randomizing a total execution time of the main program.

16. A method as defined in claim 15, wherein randomizing the total execution time comprises branching or jumping from the main program to a randomly-selected

address in a sub-program, executing the sub-program from the randomly-selected address to an instruction for returning to the main program, and resuming execution of the main program following returning from the sub-program.

17. A method as defined in claim 16, wherein the sub-program contains no instruction for jumping or branching to an address external to the sub-program, contains no infinite loop, and contains no interrupt-generating code.

18. A method as defined in claim 16, wherein the step of executing the sub-program comprises jumping or branching to a second sub-program and executing the second sub-program to the instruction for returning to the main program.

19. An integrated circuit comprising:

means for executing a main program;

means for branching or jumping from the main program to a randomly-selected address in a sub-program; and

means for executing the sub-program from the randomly-selected address to an instruction for returning to the main program.

20. An integrated circuit as defined in claim 19, further comprising means for resuming execution of the main program following returning from the sub-program.

21. An integrated circuit as defined in claim 19, wherein the means for executing the sub-program comprises means for jumping to a second sub-program and means for executing the second sub-program to the instruction for returning to the main program.

22. An integrated circuit as defined in claim 19, wherein any code in the sub-program leads directly or indirectly to the instruction for returning to the main program.